Parabola Volume 32, Issue 3 (1996)

FERMAT'S LAST THEOREM

by Michael Cowling[1]

Some 3000 years ago, the ancient Egyptians knew that the triangle with sides 3, 4 and 5 is a right-angled triangle. And of course, they also knew the related fact that $9+16 = 25$, i.e., that $3^2 + 4^2 = 5^2$.

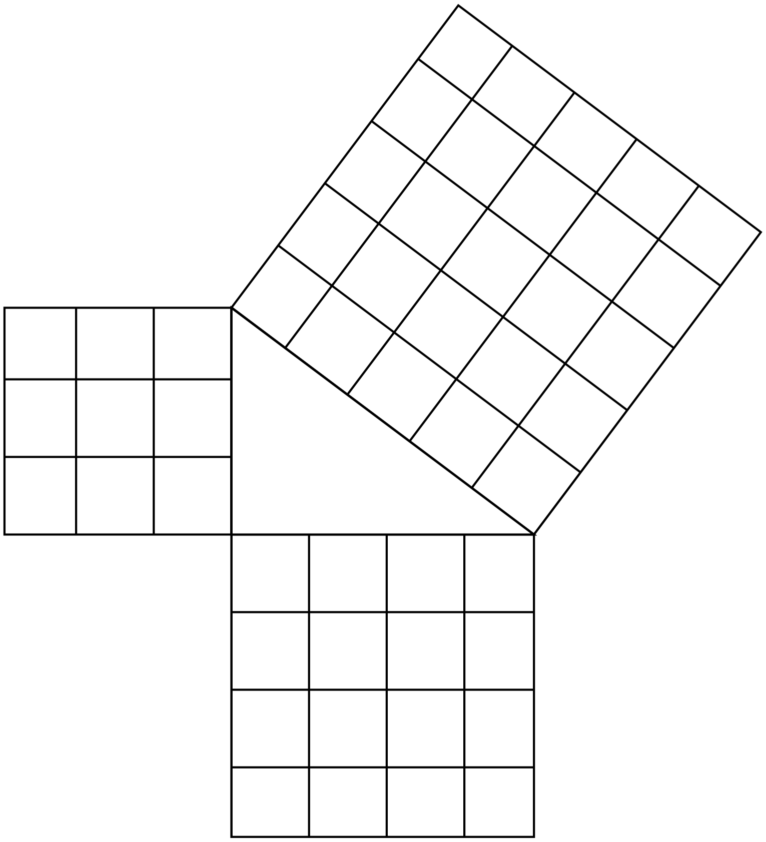


Figure 1

About 2500 years ago, Pythagoras' theorem was proved:

> *In a right angled triangle, the square on the hypotenuse is equal to the sum of the squares on the other two sides.*

[1] Michael Cowling is a Professor of Mathematics at the University of New South Wales

We say that a Pythagorean triangle is a triangle whose sides are all of integer length (in some system of measurement). A Pythagorean triple is made up of three positive integers a, b, and c such that

$$a^2 + b^2 = c^2.$$

If a, b, and c have no common factor then the triple is called primitive.

About 1800 years ago, Diophantos of Alexandria wrote a book on mathematics. One part of this (Book 2, problem 8) dealt with the problem of finding all Pythagorean triangles, or equivalently, all Pythagorean triples. Obviously, it is enough to find all primitive triples.

If a, b, and c are positive integers, and

$$a^2 + b^2 = c^2$$

then

$$(a/c)^2 + (b/c)^2 = 1.$$

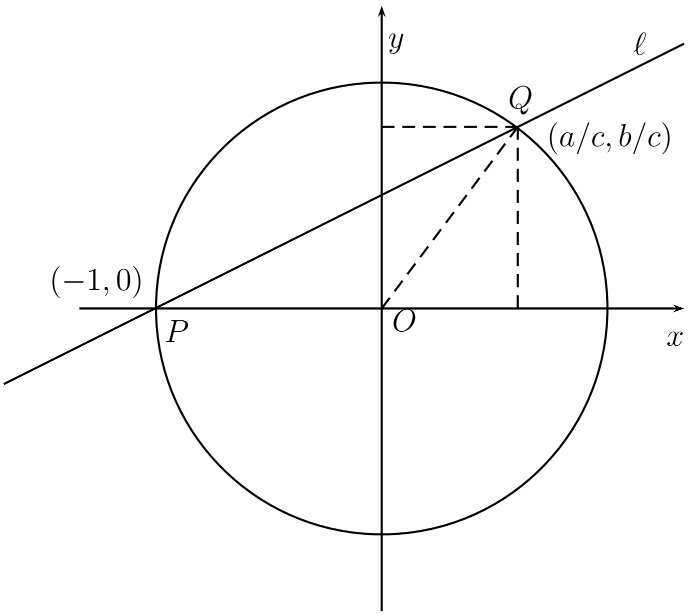


Figure 2

On a circle of unit radius, centred at the origin, we draw the line ℓ, joining the point $P(-1, 0)$ to the point $Q(a/c, b/c)$. The gradient t of the line ℓ, i.e., $\dfrac{b/c}{1 + a/c}$, is a rational number, between 0 and 1. Thus to every Pythagorean triple, we may associate a rational number t between 0 and 1. This process will associate the same rational number to all triples which are multiples of the same primitive triple.

Conversely, if ℓ is a line passing through the point P whose gradient is a rational number between 0 and 1, it meets the circle again at another point Q, whose coordinates x and y are rational numbers, also between 0 and 1. In fact, x and y may be found in terms of the gradient t of the line ℓ, by solving simultaneously the equations of the circle (i.e., $x^2 + y^2 = 1$) and of the line (i.e., $y = t(x + 1)$). It turns out that

$$x = \frac{1 - t^2}{1 + t^2} \qquad \text{and} \qquad y = \frac{2t}{1 + t^2}.$$

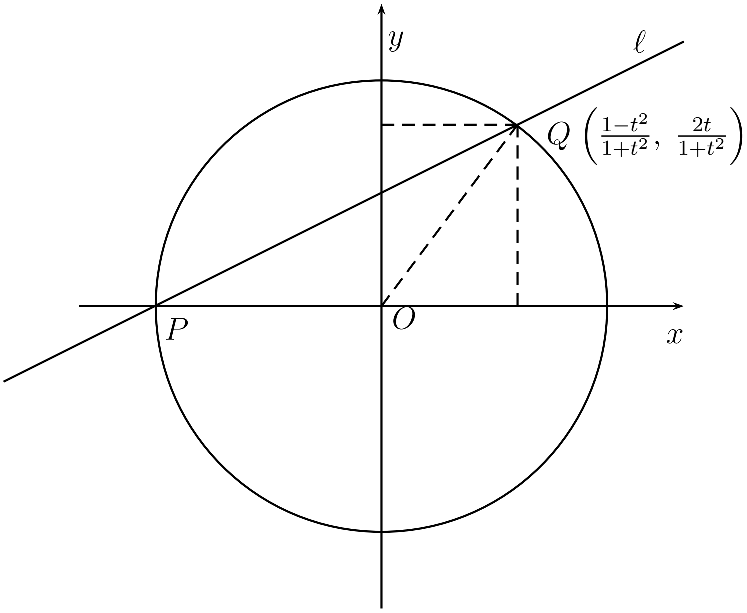


Figure 3

We write x and y as fractions, and put these fractions over a common denominator. Hence, we may find integers a, b, and c such that

$$x = a/c \qquad \text{and} \qquad y = b/c.$$

Now $(a/c)^2 + (b/c)^2 = 1$, so $a^2 + b^2 = c^2$. Thus to every rational number t between 0 and 1, we may associate a Pythagorean triple. By factoring out any common factors, we may assume that this Pythagorean triple is primitive.

By considering all possible rational numbers between 0 and 1 as gradients, we can find all possible primitive Pythagorean triples. These are of the form $(m^2 - n^2, 2mn, m^2 + n^2)$, where m and n are positive integers, where one is odd and one is even, with no common factors, and with $m > n$.

About 350 years ago, Pierre de Fermat wrote in the margin of his copy of Diophantos's book:

Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

In English, this may be translated thus:

"It is impossible to divide a cube into the sum of two cubes, or a fourth power into the sum of two fourth powers, nor generally any power higher than a square into two powers with the same exponent. I have discovered a truly marvellous proof of this. However the margin is not large enough to contain it."

Today, we paraphrase this:

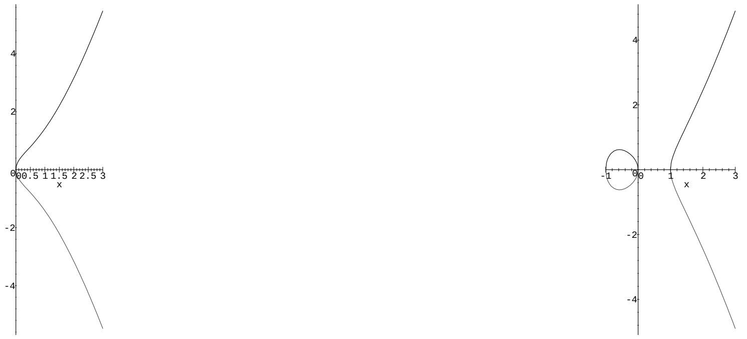
If n is an integer greater than two, it is impossible to find positive integers a, b, c such that

$$a^n + b^n = c^n.$$

It is enough to be able to show this when $n = 4$, or when n is a prime number (2, 3, 5, 7, 11, 13, 17, 19, $\ldots$). Fermat definitely did this for the case where $n = 4$, using a method called "descent". The idea is that, assuming that you can find a solution, then you can find a "smaller" one, and then a smaller one still, and then yet another one, and so on *ad infinitum*. But there cannot be infinitely many solutions all smaller than the one we started out with, so our assumption that you can find a solution, which leads to an impossible conclusion, must be wrong.

However, despite the efforts of many of the best mathematicians in the world for the next three hundred years, Fermat's mysterious proof has never been found.

In the 1900's, many mathematicians studied "elliptic curves". These are equations of degree 3 in two variables (see Figure 4 for an example).



(a) $y^2 = x^3 + x$

(b) $y^2 = x^3 - x$

Figure 4

More generally, one has an equation of the form

$$y^2 = x^3 + Ax + B$$

(where A and B are integers subject to the condition that $4A^3 + 27B^2 \neq 0$).

Some elliptic curves are said to be "modular". This is an idea involving complex numbers which is too hard to try to explain here. Out of work of Goro Shimura, Yutaka Taniyama and André Weil, the conjecture that all elliptic curves are modular emerged.

In 1982, Gerhard Frey suggested that, if all elliptic curves were modular, then Fermat's Last Theorem would be true. More precisely, if a, b, and c are positive integers, p is a prime number, and

$$a^p + b^p = c^p,$$

then the elliptic curve

$$y^2 = x(x - a^p)(x - b^p)$$

cannot be modular. So conversely, if all elliptic curves are modular, then Fermat's equation $a^p + b^p = c^p$ cannot have a solution in the positive integers.

Frey's suggestion was proved by Ken Ribet, following an approach suggested by Jean-Pierre Serre.

In 1993 Andrew Wiles announced, and in 1995 he published, a proof of Fermat's Last Theorem (with a little help from his student Richard Taylor). He didn't actually prove that all elliptic curves are modular, but he proved something close enough to it that Fermat's Last Theorem was still a consequence of it.

So, after 350 years, a chapter of Mathematics seems to have been closed—but it hasn't really. Mathematicians are still hoping to prove the Shimura–Taniyama–Weil conjecture, so we still have problems to work on.

In conclusion, as the "Space Race" led to the development of non-stick fry-pans and many other useful everyday items, so too these studies have also led to useful spin-offs. In particular, the transmission of confidential data along telephone lines and by radio requires the use of coding procedures, and elliptic curves are now used for fast and efficient coding (actually a property of these which goes back to Diophantos and Newton). So, when you use automatic tellers or EFTPOS, then it might well be that the mathematics used to tackle Fermat's problem is being used to protect you from fraud.

* * * * * * * * * *

HIGH-SPEED CALCULATION

Without your looking, ask your friend to write down any two numbers with one below the other. Now ask her to add these two numbers together and write their sum below them, then the sum of the last two numbers below that and so on, until there are ten numbrs in a column. For example, if she thought of the numbers 3 and 5, then she will have written

$$\begin{array}{r} 3\\ 5\\ 8\\ 13\\ 21\\ 34\\ 55\\ 89\\ 144\\ 233\\ \hline \end{array}$$

You now look at the numbers and, almost immediately, write down the total of these numbers (which, in the above example, is 605).

Explanation in solutions section